1-2004

A secure and privacy enhanced location-based service transaction protocol in ubiquitous computing environment

Konidala DIVYAN

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Jianying ZHOU

Kwanjo KIM

Citation

DIVYAN, Konidala; DENG, Robert H.; ZHOU, Jianying; and KIM, Kwanjo. A secure and privacy enhanced location-based service transaction protocol in ubiquitous computing environment. (2004). *SCIS 2004: Proceedings of the 2004 Symposium on Cryptography and Information Security, Sendai, 27-30 January*. 931-936. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/1088

SCIS 2004 The 2004 Symposium on
Cryptography and Information Security
Sendai, Japan, Jan.27-30, 2004
The Institute of Electronics,
Information and Communication Engineers

A Secure and Privacy Enhanced Location-based Service Transaction Protocol in Ubiquitous Computing Environment

Konidala M. Divyan [*] Robert H. Deng [†] Jianying Zhou [†] Kwangjo Kim [*]

Abstract— Nowadays mobile phones and PDAs are part and parcel of our lives. By carrying a portable mobile device with us all the time we are already living in partial Pervasive Computing Environment (PCE) that is waiting to be exploited very soon. One of the advantages of pervasive computing is that it strongly supports the deployment of Location-Based Service(s) (LBSs). In PCE, there would be many competitive service providers (SPs) trying to sell different or similar LBSs to users. In order to avail a particular service, it becomes very difficult for a low-computing and resource-poor mobile device to handle many such SPs at a time, and to identify and securely communicate with only genuine ones. Our paper establishes a convincing trust model through which secure job delegation is accomplished. Secure Job delegation and cost effective cryptographic techniques largely help in reducing the burden on the mobile device to securely communicate with trusted SPs. Our protocol also provides users privacy protection, replay protection, entity authentication, and message authentication, integrity, and confidentiality. This paper explains our protocol by suggesting one of the LBSs namely "Secure Automated Taxi Calling Service".

Keywords: Privacy protection, ubiquitous computing environment, trust model, secure job delegation, location-based services, secure mobile device communications.

1 Introduction

Pervasive computing [1][2] or Ubiquitous computing means availability of computing and communication resources whenever and wherever we are. A Pervasive Computing Environment (PCE) is saturated with devices, which compute and communicate "for", "on behalf" and "along with" the users in order to provide some useful services. The user should obtain and make use of such services seamlessly and comfortably, but should never be burdened with instructions and interfaces on how to handle those devices.

Nowadays mobile phones and PDAs are part and parcel of our lives. We are now able to communicate whenever and from wherever we are. Apart from helping us to communicate, these mobile devices would very soon allow us to interact with other smart devices around us, thus supporting an open PCE. One of the advantages of pervasive computing environment is that it would lead to the growth of new breed of service providers (SPs) who would offer Location-Based service(s) (LBSs).

Recently 3G (3rd Generation) [8][9] GPS (Global Positioning Service) enabled mobile phones [12-15] and PDAs [11] are being introduced in to the consumer market. Such mobile devices greatly assist the open PCE by allowing users to determine their location at the touch of a button, and download location specific information like graphical maps and other useful services. By sending out our current location information, SPs can provide us with services "related to" and "available at" that location.

Consider a situation where you are approaching a location, which has a food court, a movie hall, a discount store and many more shops. The mobile device on behalf of its owner may need to communicate with more than one SP. Communicating with many SPs, identifying and authenticating genuine ones, checking the validity of their digital certificates and signatures (if in case they are using Public-key Infrastructure (PKI) [7]), securing the entire transaction and protecting the owner's privacy, cannot be handled alone by the low-computing and resource-poor mobile device. It would create a huge burden on the mobile device and is certainly not user-friendly. One other feature of PCE is "job delegation" among smart devices. A low-computing device can delegate its job to a trusted high-computing device/entity.

This paper establishes a secure and privacy enhanced location-based service reservation protocol and explains the same by suggesting one of the LBSs namely "Secure Automated Taxi Calling Service".

2 LBS: A Secure Automated Taxi Calling Service

2.1 Motivation

In the current taxi calling system, the user through a telephone call directly interacts with the call center. As a result some of the call centers in order to provide quick and personalized services to returning customers, maintain travel records (travel history) and detailed profiles of its customers like their phone numbers, names, and addresses of frequently visited places (home, office, shopping malls, etc). But this is in fact privacy intrusion and violation.

2.2 Protocol Overview

Our simple, efficient and cost effective protocol addresses the above-mentioned concerns. Our protocol consists of four entities:

- Users (U)
- Trusted Proxies: Mobile Operators (MO) like AT&T, BT, Vodafone, NTT-DoCoMo, etc.

[*] International Research Center for Information Security (IRIS), Information and Communications University (ICU), 119, Munji-Ro, Yusung-Gu, Daejeon 305-714, Republic of Korea, (divyan, kkj)@icu.ac.kr

[†] Infocomm Security Group, Institute for Infocomm Research (I^2R), 21 Heng Mui Keng Terrace, Singapore 119613, (deng, jyzhou)@i2r.a-star.edu.sg

- Service Providers: Taxi Control Center (CC) and its associated Taxis (T)

A user using his GPS enabled mobile phone detects his current location and requests for a list of services available at that location. MO takes responsibility on behalf of users to select, identify, and authenticate the genuine SPs and also maintains a list of services they offer at a particular location. It updates this list as and when required. If the resource-poor mobile device had to do the above job done by MO, it would create a huge burden on it. As a result, we can notice that secure job delegation to MO plays a very critical role.

MO sends the list of available services to user's mobile phone. User selects "Taxi Calling" service from the list. He detects his current location and also identifies the destination he has to reach on an interactive map displayed in his GPS enabled mobile phone. He securely communicates these details to MO as an input to the taxi calling service. Due to this this Alice need not remember the phone numbers of many taxi call centers that operate area wise and foreigner Bob need not speak the local language to convey his current location and destination details.The communications between user and MO could be via SMS (Short Messaging Service) messages, MMS (Multimedia Messaging Service) messages, XML messages [23] or a more efficient data communication method employed by MO. The communications between the user and MO are secured by implementing cost-effective symmetric-key encryption and Manipulation Detection Code (MDC). This avoids the expensive PKI implementations and reduce the computational overhead on the mobile phone.

MO behaving like a "proxy" processes the request on behalf of the user, thus greatly reducing the burden on his mobile phone. MO identifies and authenticates the genuine SPs and securely sends only the user's current location and destination details (but not the identity of the user) to CC. This protects the privacy of the user. CC cannot maintain the user's travel record and his detailed profile, as it does not know to whom the service is being offered to. Since MO and CC are resource rich entities, the communications between them are secured by implementing PKI based encryption and digital signing.

CC, Which keeps track of all its associated taxis, securely communicates with them the current location and destination details of the user and dispatches an available taxi closest to user's current location. The communications between CC and its associated taxis are secured by implementing cost-effective symmetric-key encryption and Manipulation Detection Code (MDC). The reason being the taxis may carry resource-poor mobile devices.

2.3 Security Requirements

This section describes the various security requirements of our protocol

Users Privacy Protection: privacy is at a greater risk in PCE where users interact with many smart devices around them. Users are prone to revealing their location and identity information to such devices. This information could allow SPs to generate detailed profiles of the user, his buying interests and trace all his actions. As a result restricted access to users personal data [18] should be provided by all protocols executing in PCE.

Other security requirements include: entity authentication, replay protection, message authentication, message Integrity, and message confidentiality

3 Cryptographic Primitives

This section points out the various cryptographic primitives utilized in our protocol and related references.

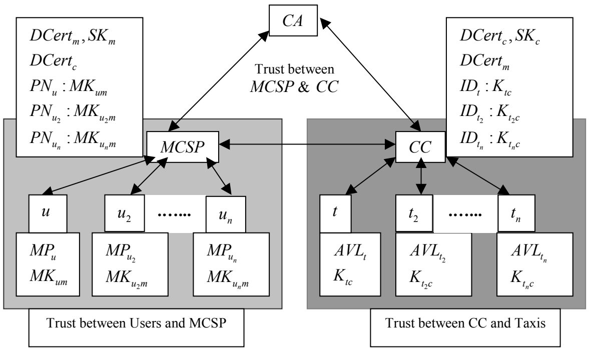

Figure 1: Trust Model and Setup Phase

Key freshness [24], Timestamps [16], Hash function [6][19][20][21], Message Authentication and integrity using a MAC [6], Message Authentication and integrity using encryption and a MDC [6].

4 Protocol Description

4.1 Notations

We state all the notations used in this paper in Tables 1&2. A brief description of an AVL system, which would be referred in the subsequent sections is as follows:

AVL System: Automatic Vehicle Location system includes Global Positioning System (GPS) with Geographical Information System (GIS). It provides precision time and position data for a vehicle or its trailer to a regional or national control center that operates and manages fleet movements. The GIS element of the AVL system provides fleet managers with on-the-spot information regarding a vehicle and its driver's whereabouts [4].

4.2 Trust Model and Setup Phase

This section describes the trust model and the setup phase needed to execute our protocol. In PCE many smart devices, which could be genuine or malicious compute and communicate with each other. To ensure secure transactions and key distribution, establishing an efficient and a convincing trust model is very much required. Also with existence of such a trust model, it would be lot easier for the mobile device to delegate their work to a nearby trusted high-computing and resource-rich entity like MO, which processes the request on behalf of the them.

Figure 1 depicts the Trust Model and the Setup Phase.

4.2.1 Trust between users and mobile operator

User installs software in his mobile phone. The software is required to execute various procedures involved in this protocol. User can either download the software through MO's official website or by approaching the nearest MO's licensed customer service center. The software helps to generate a master secret key shared between user (u) and MO (MK_{um}). MK_{um} is stored in the user's mobile phone and is also stored in the database of MO, probably with user's mobile phone number being the index or the reference for such a database entry. As a result for all users, MO generates a unique master shared secret key.

Why Trust the Mobile Operator?

In the current mobile communications paradigm we already trust MO a lot, as it handles all our voice and data communications. It maintains a record of each

Table 1: Notation

Notation	Description
MO	Mobile Operator. Establishes mobile communications network infrastructure. E.g., AT&T, BT, Vodafone, NTT-DoCoMo, etc
ID_m	Identity of MO
$DCert_m$	Digital Certificate of MO
SK_m	Private Key of MO
PK_m	Public Key of MO
U	All Subscribers of MO
u	One particular subscriber who has registered for Taxi Calling Service. $u \in U$
MP_u	GPS enabled Mobile Phone of u
PN_u	Mobile Phone Number of u. It can also be the Identity of u
$CLocn_u$	Current Location of u
$Dest_u$	Destination to be reached by u
MK_{um}	Master secret Key shared between u and MO
K_{um}	Secret session Key shared between u and MO
CC	Taxi Control Center, keeps track of all its associated taxis
ID_c	Identity of CC
$DCert_c$	Digital Certificate of CC
SK_c	Private Key of CC
PK_c	Public Key of CC
T	All the taxis associated with CC
t	One particular taxi among all the taxis, considered for easy explanation of the protocol. $t \in T$
ID_t	Identity of t
RN_t	Registration Number of t
K_{tc}	Secret Key shared between t and CC
Tmr_{tu}	Indicates the time that would be taken by t to reach $CLocn_u$
Sid_x	Unique Service ID of service x
TR_{id}	Transaction Reference ID, which is Unique and Randomly generated for every new LBS transaction
r_y	y -th Unique Random Number
ts_{x_y}	y -th Timestamp generated by an entity x
Ack_1	Your request is being processed, please wait
Ack_2	The following taxi has been dispatched
$M_{x_y} = \{m\}$	y-th Message m sent in open by an entity x. This message is visible to everyone connected to the network
$PkiS_{SK_x}(M)$	Public Key based digital Signature function on message M with private key of an entity x
$PkiE_{PK_x}(M)$	Public Key based Encryption function on message M with public key of an entity x
$SymE_{K_{xy}}(M)$	Symmetric Key based Encryption function on message M with secret key shared between an entity x and y
$H()$	One Way Hash Function like SHA-1 (Secure Hash Algorithm) [19], [21]
$H(M)$	Hash value or message digest of a message M
$H_{K_{xy}}(M)$	Keyed Hash function on message M with secret key shared between an entity x and y

subscriber's call details (incoming and outgoing call numbers, talk time, etc), contact information (home and office addresses, etc), social security number, bank account and credit card details, etc. It even has the capability to easily determine our current location and tap in to our communications. But what protects us from MO turning hostile is that it has to very strictly adhere to and follow legal, security and privacy policies imposed by the law. Thus so far we have little problems in trusting MO. Our protocol extends this trust in MO to secure LBS transactions. This approach is very practical and easily deployable, as the current mobile communications infrastructure is widely spread and highly stable.

It is very convenient for mobile device to trust one single entity like MO rather than validating many SPs and then trusting them. It is desirable to have our details like preferences and requests passed on to one single trusted entity rather than having our details stored with many SPs, who may be genuine or malicious.

4.2.2 Trust between mobile operator and taxi control center

For commercial gains both MO and taxi control center (CC) sign a business contract and mutually agree to provide this Automated Taxi Calling Service. A similar deal can be made with other SPs, whom MO trusts. To secure the communications between MO and CC during the protocol execution we assume the existence of a trusted Public Key Infrastructure (PKI). MO obtains digital certificate ($DCert_m$) and private key (SK_m). Similarly CC also obtains $DCert_c$ and SK_c from a Certificate Authority (CA). We assume that MO and CC have large computing resources. During the protocol execution they can easily, and very efficiently perform expensive tasks like public-key encryption, decryption, and digital certificate and signature verifications. MO stores $DCert_c$ and CC Similarly stores and $DCert_m$.

4.2.3 Trust between taxi control center and taxis

Taxi control center (CC) keeps track of all its associated taxis (T). CC generates secret Key (K_{tc}) shared between each taxi (t) and CC, which will be used for securing the communications between them. K_{tc} can be stored in the AVL system available in the taxi and is also stored in the database of CC, probably with identity of taxi (ID_t) being the index or the reference for such a database entry. As a result all taxis receive a unique shared secret key generated by CC.

4.2.4 Analysis

One may feel that, by solely utilizing PKI implementations throughout the protocol we can avoid considerable overhead involved in managing the unique shared keys of all taxis and users at MO and CC respectively. But since MO and CC are assumed to have large computing resources, storing large number of shared secret keys would not be much of a burden on them. Also, this model avoids the expensive PKI implementations at users and at taxis, as they carry low-computing and resource-poor devices. It is very well proved in [5] that symmetric key implementations are much simpler, faster and less computationally expensive than PKI implementations.

4.3 Periodic Taxi Information Update Phase

All taxis via the AVL system periodically and continuously communicate certain details with CC. This frequently sent update information includes identity of the taxi (ID_t), availability status (vacant or not), and current location, etc. Currently most of the Taxi Calling Service Agencies employ this method of keeping track of their associated taxis. CC stores this update

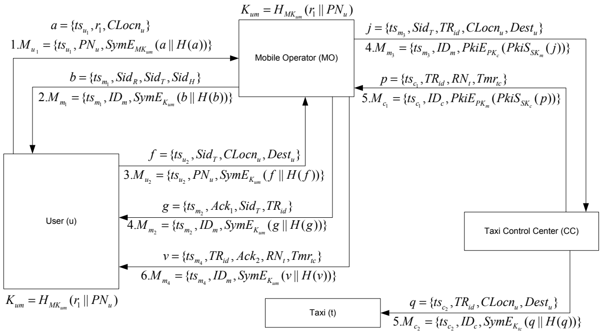
$K_{um} = H_{MK_{um}}(r_1 \| PN_u)$
$a = \{ts_{u_1}, r_1, CLocn_u\}$
$1.M_{u_1} = \{ts_{u_1}, PN_u, SymE_{MK_{um}}(a \| H(a))\}$
Mobile Operator (MO)
$j = \{ts_{m_3}, Sid_T, TR_{id}, CLocn_u, Dest_u\}$
$4.M_{m_3} = \{ts_{m_3}, ID_m, PkiE_{PK_c}(PkiS_{SK_m}(j))\}$
$b = \{ts_{m_1}, Sid_R, Sid_T, Sid_H\}$
$2.M_{m_1} = \{ts_{m_1}, ID_m, SymE_{K_{um}}(b \| H(b))\}$
$p = \{ts_{c_1}, TR_{id}, RN_t, Tmr_{tc}\}$
$5.M_{c_1} = \{ts_{c_1}, ID_c, PkiE_{PK_m}(PkiS_{SK_c}(p))\}$
$f = \{ts_{u_2}, Sid_T, CLocn_u, Dest_u\}$
$3.M_{u_2} = \{ts_{u_2}, PN_u, SymE_{K_{um}}(f \| H(f))\}$
User (u)
$g = \{ts_{m_2}, Ack_1, Sid_T, TR_{id}\}$
$4.M_{m_2} = \{ts_{m_2}, ID_m, SymE_{K_{um}}(g \| H(g))\}$
Taxi Control Center (CC)
$v = \{ts_{m_4}, TR_{id}, Ack_2, RN_t, Tmr_{tc}\}$
$6.M_{m_4} = \{ts_{m_4}, ID_m, SymE_{K_{um}}(v \| H(v))\}$
$K_{um} = H_{MK_{um}}(r_1 \| PN_u)$
Taxi (t)
$q = \{ts_{c_2}, TR_{id}, CLocn_u, Dest_u\}$
$5.M_{c_2} = \{ts_{c_2}, ID_c, SymE_{K_{tc}}(q \| H(q))\}$

Figure 2: User LBS Request Processing Phase

information in its database with ID_t being the index or the reference for such entries.

4.4 Request Processing Phase

Figure 2 depicts this phase.

4.4.1 STEP 1

User (u) enters the secret PIN (Personal Identification Number) to authenticate himself to his mobile phone. This prevents unauthorized communications in the event his mobile phone is stolen or being tampered with. The above option is currently available in all the mobile phones. User, using his GPS enabled mobile phone detects his current location ($CLocn_u$). User, using the master shared secret key MK_{um} performs symmetric-key encryption and MDC on message M_{u_1} and sends it to MO. M_{u_1} contains a request for a list of available services at $CLocn_u$. User also generates a session key K_{um} using a keyed hash function of a unique random number (r_1) concatenated with his mobile phone number (PN_u).

$$a = \{ts_{u_1}, r_1, CLocn_u\}$$

$$M_{u_1} = \{ts_{u_1}, PN_u, SymE_{MK_{um}}(a||H(a))\}$$

$$K_{um} = H_{MK_{um}}(r_1||PN_u)$$

Security Analysis

Entity Authentication, Message Authentication, Integrity, and Confidentiality: The above equation provides entity Authentication, message authentication, integrity, and confidentiality by utilizing symmetric-key encryption and Manipulation Detection Code (MDC).

Replay Protection: Unlike wire-based communication systems where lines can be put up until they obliterate the sky, each wireless system requires its own unique slice of the limited radio spectrum. In order to get the most out of its assigned slice of the radio spectrum, a wireless system must be carefully timed and synchronized [22]. As a result in the current mobile communications scenario (like TDMA technology) the clock of the mobile phones are synchronized with the clock of MO. This aspect greatly supports the use of timestamp [16] as nonce to prevent replay attacks.

Key Freshness: Long-term master key MK_{um} is used only once at the beginning of the session to prevent key compromise due to extensive use. Instead MK_{um} is used to generate a short-term session key K_{um}. K_{um} is used to protect the rest of the communications between the user and MO for that particular session only.

4.4.2 STEP 2

MO receives M_{u_1} and also the phone number of the user (PN_u) as a part of the incoming message information from STEP 1. MO checks PN_u and retrieves the corresponding MK_{um} from its database and decrypts M_{u_1}. MO obtains r_1 and $CLocn_u$. Using r_1, PN_u, and MK_{um}, MO generates the session key K_{um}. Using K_{um}, MO performs symmetric-key encryption and MDC on message M_{m_1} and sends it to the user. M_{m_1} contains a list of services available at $CLocn_u$.

$$K_{um} = H_{MK_{um}}(r_1||PN_u)$$

$$b = \{ts_{m_1}, Sid_R, Sid_T, Sid_H\}$$

$$d = \{b||H(b)\}$$

$$M_{m_1} = \{ts_{m_1}, ID_m, SymE_{K_{um}}(d)\}$$

4.4.3 STEP 3

User's mobile phone receives message M_{m_1} from STEP 2. Mobile phone checks ID_m and retrieves the recently generated K_{um} and decrypts M_{m_1}. M_{m_1} can be displayed as follows in the mobile phone:

The list of services available at $CLocn_u$ is
Sid_R: Restaurant Information Service
Sid_T: Taxi Calling Service
Sid_H: Hotel Information Service
Please Select your choice

Since user requires Taxi Calling Service, he selects Sid_T. User using his GPS enabled mobile phone detects $CLocn_u$ and identifies the destination $Dest_u$ to be reached on an interactive map displayed in the mobile phone. Using K_{um}, user performs symmetric-key encryption and MDC on message M_{u_2} and sends it to the MO. M_{u_2} contains a service ID selected by the user and other information related to that service like $CLocn_u$ and $Dest_u$.

$$f = \{ts_{u_2}, Sid_T, CLocn_u, Dest_u\}$$

$$M_{u_2} = \{ts_{u_2}, PN_u, SymE_{K_{um}}(f||H(f))\}$$

4.4.4 STEP 4

MO receives M_{u_2} and decrypts it using K_{um}. MO checks the user's preference as taxi calling service (Sid_T). MO creates a unique random transaction ID (TR_{id}) for this particular LBS transaction. Unique TR_{id}, plays a vital role in identifying one entire Taxi Calling Service transaction for the user. Using K_{um}, MO sends message M_{m_2} to the user. M_{m_2} contains TR_{id}, Sid_T and an acknowledgement to the user stating that his request is being processed.

$Ack_1 =$ Your request is being processed, please wait

$$g = \{ts_{m_2}, Ack_1, Sid_T, TR_{id}\}$$

$$M_{m_2} = \{ts_{m_2}, ID_m, SymE_{K_{um}}(g||H(g))\}$$

User receives M_{m_2} from STEP 4. Mobile phone (MP_u) using K_{um} decrypts M_{m_2}. MP_u obtains TR_{id}. User can now use TR_{id} as a reference to easily and quickly cancel this request or update his current location at a later stage (before the taxi could reach him).

MO using its private-key (SK_m) and CC's public-key (PK_c) sends a PKI based encrypted signed message M_{m_3} to CC. M_{m_3} contains service ID, its corresponding transaction ID, current location and destination details of the user. It can be noticed that identity of the user like his phone number is never sent to CC and therefore CC can never know whose location details are being sent. This protects the privacy of the user. Its TR_{id}, which identifies this transaction. In the current call taxi scenario, user's phone number, his name or address is used to identify the transaction leading to privacy intrusion.

$$j = \{ts_{m_3}, Sid_T, TR_{id}, CLocn_u, Dest_u\}$$
$$M_{m_3} = \{ts_{m_3}, ID_m, PkiE_{PK_c}(PkiS_{SK_m}(j))\}$$

Security Analysis

Entity Authentication, Message Authentication, Integrity, and Confidentiality: According to our Trust Model, MO and CC have enough computing resources to carry out expensive PKI implementations. Public-key based implementations like encryption and digital signature provide entity authentication, message authentication, integrity, and confidentiality.

4.4.5 STEP 5

CC receives M_{m_3}, and decrypts it using its private-key (SK_c) and verifies the signature. Now CC knows the current location of the user $CLocn_u$ and the destination he has to reach $Dest_u$. By comparing $CLocn_u$ and already available current location details of all its associated taxis (via the Periodic Taxi Information Update Phase), CC detects, selects and dispatches a taxi (t) that is nearest to $CLocn_u$. CC updates its database by including some of the reserved taxi's details like registration number (RN_t), driver's name, date, and time, probably with TR_{id} being the index or the reference for such an entry. This database entry may be used as a receipt for this particular transaction or for any payment transactions at a later stage. CC using its private-key (SK_c) and MO's public-key (PK_m) sends an PKI based encrypted signed message M_{c_1} to MO. M_{c_1} contains identity of CC, TR_{id}, registration number of the reserved taxi (RN_t) and the time taken by t to reach $CLocn_u$ (Tmr_{tu}).

$$p = \{ts_{c_1}, TR_{id}, RN_t, Tmr_{tc}\}$$
$$M_{c_1} = \{ts_{c_1}, ID_c, PkiE_{PK_m}(PkiS_{SK_c}(p))\}$$

Simultaneously, CC using the shared secret key K_{tc} performs symmetric-key encryption and MDC on message M_{c_2} and sends it to the reserved taxi (t). Through M_{c_2}, TR_{id}, $CLocn_u$, and $Dest_u$ are securely communicated to t.

$$q = \{ts_{c_2}, TR_{id}, CLocn_u, Dest_u\}$$
$$M_{c_2} = \{ts_{c_2}, ID_c, SymE_{K_{tc}}(q||H(q))\}$$

t receives M_{c_2}, checks for ID_c and retrieves the corresponding K_{tc}. Using K_{tc}, t decrypts M_{c_2}. Now t knows the $CLocn_u$, and $Dest_u$, which are sufficient to pick up the user from his current location.

4.4.6 STEP 6

MO receives M_{c_1} from STEP 5 and decrypts it using its private-key SK_m and verifies the signature on M_{c_1}. MO checks for the received TR_{id} in its database and retrieves the corresponding user's mobile phone number and recently generated session key K_{um}. Using K_{um}, MO sends message M_{m_4} to the user. M_{m_4} contains an acknowledgement stating that a taxi has been dispatched, identity of CC, TR_{id}, registration number of the reserved taxi (RN_t) and the time taken by t to reach $CLocn_u$ (Tmr_{tu}).

Ack_2 = The following taxi has been dispatched

$$v = \{ts_{m_4}, TR_{id}, Ack_2, RN_t, Tmr_{tc}\}$$
$$w = \{v||H(v)\}$$
$$M_{m_4} = \{ts_{m_4}, ID_m, SymE_{K_{um}}(w)\}$$

User receives M_{m_4}. Using K_{um} he decrypts M_{m_4}. User stores TR_{id}, and RN_t, which can used as a receipt for this particular transaction or for any payment transactions at a later stage. User reads Tmr_{tc} and waits for the reserved taxi t.

Security Analysis The security analysis done at STEP 1, 2, & 4 holds good for this STEP. Additional analysis is as below.

Privacy Protection It can be noticed that TR_{id} is never sent in open. It is always well encrypted and securely communicated among the four entities. In the current taxi calling scenario identity of (e.g., name, or phone number) the user is used to identify one entire transaction. This does not protect user's privacy. Whereas in our protocol a unique TR_{id} is used to identify one unique transaction, thus protecting user's privacy.

4.5 Pickup Phase

Reserved taxi (t) reaches curent location of the user. User has already obtained the registration number of the reserved taxi (RN_t) via the message M_{m_4}. The message M_{m_4} has been securely communicated to the user. Looking if registration number of the arrived taxi equals RN_t, user can identify, authenticate and trust the arrived taxi as t else the arrived taxi is not the right taxi dispatched by CC.

5 Comparison with Related Works

Most of the pervasive computing projects [27-30] being carried out at various universities and research institutes deal in closed pervasive computing environments (PCE) like home networking or Smart Spaces in buildings. In such closed environments, interacting smart devices are mostly under the control of a trusted server (for e.g., a home server) and with establishment of proprietary trust model every device can easily trust and communicate with every other device. Key distribution, access control, privacy protection and security policies for securing the communications can be easily accomplished in such closed environments.

But in an open PCE (for e.g., streets, highways, etc.) the scenario is completely different Our protocol suggests a convincing trust model in such environments to assist in key distribution, access control, privacy protection and secure communication. [18] [23] [25] [26] [30-34] describe the need and importance of privacy protection in PCE and LBSs and also suggest privacy protection methods, which can be broadly categorized as follows:

5.1 Identity Management [26]:

In this method users interact with other smart devices through pseudonyms. [31] describes the drawbacks of this method. The user has to choose carefully, towards which party he uses which VID and when he has to change this VID. This approach creates burden on the user's mobile device to decide and choose the appropriate VID depending on the interacting SP.

5.2 Adhering to the privacy policies issued by the law [32] [34]:

[35] describes the drawbacks of adhering to privacy policies approach. In this scenario, resource-rich mobile operator can make sure that the SPs are adhering to the policies by verifying their claims on behalf of the user's mobile devices.

5.3 Use of Proxies:

According to [23] the proxy can conceal from the SP the mobile device's mobileID and protect its identity. But the paper fails to mention about how to establish or envisage such a trusted proxy. Our paper clearly justifies the consideration of MO to be such a trusted proxy. In our protocol the mobile device neither stores a list of trusted SPs nor their corresponding keys.

6 Conclusion

The advantages of this protocol are as follows: Simple, involves less user interactions, involves secure delegation of duties among the entities, automation leads to speedy taxi calling service as it involves less human interactions, in case of a legal inquiry the entire transaction can traced using TR_{id}, the taxi control center cannot maintain users travel record and their profiles because they would never know the users phone number, this protects users privacy, TR_{id} speeds up the process of cancellation of a request and current location update of walking users, avoids expensive PKI implementations at user end and at taxis end as they have low-computing and resource-poor mobile devices, automation reduces the cost involved in establishing taxi call centers and manpower to manage them.

There are many advantages of Secure Automated Taxi Calling Service and could be a killer application as it speeds up the call taxi process. This facility would be greatly sought by both public and taxi drivers. For public it could be a quick, useful and convenient service, which also protects their privacy. For the taxi drivers, they would never pass by a waiting customer unnoticed. This could mean more money to them. It could be a good revenue generator for the mobile operators and the taxi call center through commissions for every transaction.

Finally this protocol adheres to pervasive computing requirements, as there is a secure delegation of work between low-computing devices and high-computing devices. The user passes on his request to the trusted MO, which then identifies and authenticates the genuine service providers, and establishes a secure communication with them on behalf of the user. As a result the mobile device can securely handle many service providers at a time. The load on the users mobile phone is greatly reduced by employing cheap yet strong cryptographic techniques like hash functions, message authentication and integrity using symmetric-key encryption and a MDC in order to secure the communication channel. This protocol would certainly serve the purpose for most of the Location-Based Services in open pervasive computing environment.

References

[1] M. Weiser, "The Computer for the 21st Century", Sci. Amer., Sept., 1991

[2] M. Satyanarayanan, "Pervasive Computing: Vision and Challenges", IEEE Personal Communications, August 2001

[3] National Institute of Standards and Technology (NIST),"Pervasive Computing SmartSpace Laboratory"

[4] S.M. Dye, Dr. F. Baylin, "Mobile Positioning", published by Mobile Life streams, 1999

[5] A.M. Basyouni and S.E. Tavares,"Public Key versus Private Key in Wireless Authentication Protocols", Proceedings of the Canadian Workshop on Information Theory, Toronto, June 1997

[6] A.J. Menezes, P.C. vaz Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, Chapter 9, Hash Functions and Data Integrity, CRC Press.

[7] Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, IT-22(6):644-654, Nov 1976.

[8] Introduction to 3G, http://www.3g.co.uk/All About 3G.htm

[9] 3rd Generation Partnership Project (3GPP), http://www.3gpp.org/

[10] Global positioning system overview and bibliography, http://www.colorado.edu/

[11] Garmins iQue 3600, the first PDA to include integrated GPS technology

[12] Samsung GPS-enabled SPH-N300 Wireless Phone

[13] Motorolas GPS enabled i205 Handset

[14] NTT DoCoMos first Global Positioning Service (GPS)-compatible handset F661i

[15] SiRFs GPS chip sets, http://www.sirf.com/products.html

[16] A.J. Menezes, P.C. vaz Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, Chapter 10,Identification and Entity Authentication, CRC Press.

[17] David Youd, "An introduction to Digital Signatures", http://www.youdzone.com/signature.html

[18] H.T. Tavani, and J.H. Moor,"Privacy Protection, Control of Information, and Privacy-Enhancing Technologies", ACM SIGCAS Newsletter. 2001.

[19] William Stallings, "Secure Hash Algorithm", in Cryptography and Network Security: principles and practice Second Edition, Prentice-Hall.

[20] Bruce Schneier, "Using One-Way Hash Functions", in Applied Cryptography Second Edition, John Wiley & Sons,Inc.

[21] National Institute of Standards and Technology, "Secure Hash Standard", FIPS Publication 180-1, 1995

[22] Peter Kuykendall and Dr. Peter V. W. Loomis, Trimble Navigation, "In Sync with GPS: GPS Clocks for theWireless Infrastructure".

[23] Escudero A., Maguire G.Q.,"Role(s) of a proxy in location based services", PIMRC2002, Portugal, Sep 2002.

[24] A.J. Menezes, P.C. vaz Oorschot, S.A. Vanstone, "Handbook of Applied Cryptography", Chapter 12,Key Establishment Protocol, CRC Press

[25] S. Lederer, J. Mankoff, A. Dey," Towards a Deconstruction of the Privacy Space", Ubicomp'2003.

[26] U. Jendricke, M. Kreutzer and A. Zugenmaier,"Pervasive Privacy with Identity Management", UBICOMP 2002.

[27] MIT Project Oxygen, http://oxygen.lcs.mit.edu/.

[28] Easy Living, Microsoft Research, http://research.microsoft.com/easyliving/.

[29] The Aware Home, Georgia Institute of Technology, http://www.cc.gatech.edu/fce/ahri/.

[30] GAIA - Active Spaces for Ubiquitous Computing, University of Illinois at Urbana-Champaign.

[31] Christian Hauser, "Privacy and Security in Location-Based Systems With Spatial Models", PAMPAS'02.

[32] G. Myles, A. Friday, and N. Davies, "Preserving Privacy in Environments with Location-Based Applications", IEEE Pervasive Computing journal, Jan-Mar 2003.

[33] A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing", IEEE Pervasive Computing journal, Jan-Mar 2003.

[34] Marc Langheinrich , "A Privacy Awareness System for Ubiquitous Computing Environments",

[35] Moamo Wu, Adrian Friday, "Integrating Privacy Enhancing Services in Ubiquitous Computing Environments", UBICOMP2002